No. 2197 Registered No. N. E. 930.

TRIPURA GAZETTE

Published by Authority

EXTRAORDINARY ISSUE

Agartala, Monday, December 1, 2025 A. D., Agrahayana 10, 1947 S. E.

PART--I-- Orders and Notifications by the Government of Tripura, The High Court, Government Treasury etc.

GOVERNMENT OF TRIPURA

DEPARTMENT OF INDUSTRIES & COMMERCE

(INFORMATION TECHNOLOGY)

No.F.17(11)/DIT/CSP/2025/ **Dated, 23rd November, 2025.**

NOTIFICATION

Subject: - Introduction of "Tripura Cyber Security Policy, 2025 (TCSP 2.0)".

The Governor of Tripura is pleased to approve the "Tripura Cyber Security Policy, 2025 (TCSP 2.0)" as per the details appended with this notification.

2. **Title of the Policy:** Tripura Cyber Security Policy, 2025 (TCSP 2.0).

3. **Duration of the Policy:** The Tripura Cyber Security Policy, 2025 (TCSP 2.0) shall be applicable in the State from the date issue of this notification, until substituted by another policy/ notification/order in this regard.

4. **Salient features of the Policy:** The policy is anchored in the foundational principles of Confidentiality, Integrity and Availability (CIA) ensuring a robust and trustworthy digital environment for the Citizens, Businesses and Government. The salient features of the Policy are summarized below:

(i) Cyber Security Architecture Framework Tripura (CSAF-Tr) to define the overall ambit of cyber security-related bodies/agencies in the State,

(ii) State Level Cyber Security Steering Committee (SLCSSC) to provide strategic oversight, policy guidance and coordination,

(iii) Strengthening Legal & Regulatory Framework to address specific legislation governing cyberspace activity,

(iv) Establishment of Computer Security Incident Response Team-Tripura (CSIRT-Tr) for responding to major cyber threats,

(v) Protection of Critical Information Infrastructure (CII) of the State,

(vi) Establishment of Cyber Security Standards & Practices across the State,

(vii) Capacity Building framework for Government employees, businesses and citizens,

(viii) Collaboration framework to boost research in the field of cyber security.

By order of the Governor,

Signed by Kiran Kumar Dinkrao Gitte
Date: 23-11-2025 09:08:18

(Kiran Gitte, IAS)
Secretary to the Govt. of Tripura

RESTRICTED DOCUMENT

1. DEFINITIONS

1.1. **Critical Information Infrastructure:** Critical Information Infrastructure (CII) is defined as a computer system/resource including Operational Technology (OT) and Industrial Control Systems (ICS), the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

1.2. **Cyber Crime:** Cyber-crime is defined as a crime in which a computer system is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cyber-crimes range from basic crimes such as online harassment to calculated attacks such as fraud and financial crimes.

1.3. **Cyber Crisis Management Plan:** A strategic framework for effective cyber security incident detection, incident management and incident response.

1.4. **Cyber extortion:** Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers, who demand money in return for stopping the attacks and for offering protection.

1.5. **Cyber harassment:** Any form of harassment, such as directing obscenities and derogatory comments at specific individuals, committed through the use of computer system/resources can be categorized as cyber harassment.

1.6. **Cyber Security:** The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

1.7. **Departments/Organizations/Agencies etc.:** Administrative unit functioning under the purview of the Government of Tripura.

1.8. **Security Audit:** A periodic and comprehensive review and analysis of the IT infrastructure of an entity to identify vulnerabilities in relation to cyber security.

1.9. **Cyber Security Standards:** Techniques, best practices and/or certifications adopted to protection IT infrastructure from cyber threats. Cyber security standards are often adopted on a large scale to bring uniformity to industry on a national or global level.

1.10. **Cyber Space:** Cyber space is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

1.11. **Cyber Terrorism:** Any act of terrorism committed through the use of cyber space or computer resources can be categorized as cyber terrorism.

1.12. **Fraud and Financial Crimes:** Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss.

1.13. **Incident:** A Security event that changes or affects the everyday operations of an information technology service, indicating that a security measure may have been violated or a security safeguard may have failed.

1.14. **Information Security:** Practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

1.15. **Nodal Body/Agency:** A designated centralized body/agency to coordinate, implement and monitor policy activities related to cyber security within the State.

1.16. **Obscene or offensive content:** Delivering obscene and offensive content to users through the use of cyberspace or computer resources is considered an offense in many countries across the globe. The extent to which these communications are unlawful vary greatly based on the nation.

1.17. **Tripura-based Start-Ups:** Start-Ups registered under Tripura Start-Up Policy, 2024 and operating in Tripura.

1.18. **Tripura-based Industries:** Industries registered under Tripura Industrial Investment Policy or IT/ITeS Policy or any other related Policy of Government of Tripura are considered as Tripura-based industries that operate or manufacture goods within the State, utilizing local resources, workforce or infrastructure and contributing to Tripura's economic growth.

All other words and expressions used but not defined in this policy, but defined in the Information Technology Act, 2000 (and amendment 2008) or National Cyber Security Policy 2013 and guidelines and / or rules and regulations made there under shall have the same meaning respectively assigned to them in such Acts and / or policy and / or guidelines and / or rules regulations, as the case may be.

2. ABBREVIATIONS

2.1.	**API**	- Application Programming Interface
2.2.	**BCP**	- Business Continuity Plan
2.3.	**CCMP**	- Cyber Crisis Management Plan
2.4.	**CERT-In**	- Computer Emergency Response Team - India
2.5.	**CII**	- Critical Information Infrastructure
2.6.	**CIA**	- Confidentiality, Integrity, Availability
2.7.	**CISO**	- Chief Information Security Officer
2.8.	**CoE**	- Centre of Excellence
2.9.	**CSAF-Tr**	- Cyber Security Architecture Framework-Tripura
2.10.	**CSCs**	- Common Service Centers
2.11.	**CSIRT-Tr**	- Computer Security Incident Response Team-Tripura
2.12.	**CSOC**	- Cyber Security Operations Centre
2.13.	**DIT**	- Directorate of Information Technology
2.14.	**DR**	- Disaster Recovery
2.15.	**Dy. ISO**	- Deputy Information Security Officer
2.16.	**G2B**	- Government to Business
2.17.	**G2C**	- Government to Citizen
2.18.	**G2G**	- Government to Government
2.19.	**GIGW**	- Guidelines for Indian Government Websites
2.20.	**ICT**	- Information and Communication Technology
2.21.	**ICS**	- Industrial Control System
2.22.	**IT**	- Information Technology
2.23.	**I4C**	- Indian Cyber Crime Coordination Centre
2.24.	**ISO**	- Information Security Officer
2.25.	**MeitY**	- Ministry of Electronics and Information Technology
2.26.	**NCCC**	- National Cyber Coordination Centre
2.27.	**NCIIPC**	- National Critical Information Infrastructure Protection Centre

RESTRICTED DOCUMENT

2.28.	**NIC**	- National Informatics Centre
2.29.	**NIC-CERT**	- NIC-Computer Emergency Response Team
2.30.	**OEM**	- Original Equipment Manufacturer
2.31.	**OT**	- Operational Technology
2.32.	**PPP**	- Public Private Partnership
2.33.	**R&D**	- Research and Development
2.34.	**SAaaS**	- Security Audit as a Service
2.35.	**SDLC**	- Software Development Life Cycle
2.36.	**SLCSSC**	- State Level Cyber Security Steering Committee
2.37.	**SOC**	- Security Operation Centre
2.38.	**SOP**	- Standard Operating Procedure
2.39.	**SWAN**	- State Wide Area Network
2.40.	**TSDC**	- Tripura State Data Centre
2.41.	**TSFSL**	- Tripura State Forensic Science Laboratory
2.42.	**TSOC**	- Tripura Security Operation Centre
2.43.	**VAPT**	- Vulnerability Assessment and Penetration Testing

3. PREAMBLE

Cyberspace represents a complex and dynamic environment where individuals, enterprises, applications and services continuously interact through a vast network of ICT. This shared digital ecosystem is widely utilized by citizens, businesses, critical infrastructure sectors and Government Departments, institutions making it both indispensable and vulnerable at the same time. Ensuring a safe cyberspace is of paramount importance to the Government of Tripura, which has implemented various ICT based projects across the Government Departments and Organizations for delivering different G2G, G2B and G2C services of the State. Also, SWAN & its horizontal extensions have been extended up to Block level, along with the initiation of last mile connectivity projects. The Government has been a key driver for increased adoption of IT-based products and IT enabled services such as e-office implementation upto Gram Panchayat Level, e-cabinet, e-bidhan etc., which has led to the creation of digital public infrastructure.

In today's interconnected world, cyber security has become a cornerstone of effective governance. With the rapid expansion of e-governance initiatives, Government Departments and Organizations are generating, storing and exchanging unprecedented volumes of data, making them prime targets for malicious actors. Protecting Government networks and data from cyber threats is crucial to ensure continuity in Governance, citizen trust and uphold the credibility of public institutions.

The Government of Tripura acknowledges the vital role of cyber security in enabling a safe and resilient digital environment and is focused on adopting all possible measures to deal with cyber threats. A robust Cyber Security policy is essential to counter a wide spectrum of risks including denial of services, identity & data theft, financial frauds, privacy breaches and evolving cyber threats.

In recognition of the evolving cyber threat landscape and in alignment with the National Cyber Security Policy, the Government of Tripura has undertaken a review of its existing Cyber Security Policy released in 2018 and hereby introduces the **"Tripura Cyber Security Policy, 2025" (TCSP 2.0)**, aimed at strengthening digital resilience, enhancing preparedness and safeguarding the interests of citizens, enterprises and Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of the State's IT and ICT systems. The policy provides an overview to effectively protecting information, information systems & networks and also offers an insight into the Government's approach to enabling collaborative work with all key players in public & private sectors.

4. SCOPE

The Tripura Cyber Security Policy 2025 (TCSP 2.0) is comprehensive and applies to all Departments, State Public Sector Units, Bodies, Agencies, Organisations under the Government of Tripura that utilize IT infrastructure, networks or digital data. Additionally, the TCSP 2.0 extends to relevant stakeholders and third parties to achieve a safe and resilient cyber space for Citizens, Businesses and Government.

5. MISSION

To build a safe, secure and resilient digital ecosystem in Tripura by safeguarding Citizens, Businesses and Government against cyber threats, enhancing capabilities to prevent and respond to such threats and raising awareness to reduce vulnerabilities and minimize the impact of incidents, thereby strengthening trust in Government digital services. This mission will be achieved through effective institutional mechanisms, robust processes, technological adoption, capacity building and the active participation of responsible individuals and collaborative efforts.

6. OBJECTIVES

6.1. To safeguard Government information assets including IT & ICT infrastructure, Operational Technology (OT), Industrial Control Systems (ICS), network, software & citizen services and ensure their maximum availability to the Citizens, Businesses and Government.

6.2. To create a secure cyber ecosystem in the State, generate adequate trust and confidence in IT systems & transactions in cyberspace and thereby encouraging adoption of secured IT and ICT infrastructure in all sectors of the economy of the State.

6.3. To implement the Cyber Security Policy for Government of Tripura, under a suitable framework for promotion and enabling actions for compliance towards the national & global standards and best practices.

6.4. To establish a nodal body for the State to coordinate with Departments, institutions, organizations &agencies which will contribute towards the State's efforts for a safer, stronger & trusted Internet for all citizens by responding to major incidents, analysing threats and exchanging critical cyber security information with trusted partners.

6.5. To strengthen the Legal and Regulatory framework for ensuring a secure cyberspace ecosystem and to foster cooperation and coordination with other cyber

security agencies and institutions such as MeitY, CERT-In, NCIIPC, NCCC, I4C, NIC-CERT, Cyber Crime Unit, SFSL etc.

6.6. To enable effective prevention, investigation and prosecution of cyber-crime with a quantifiable increase from a base line figure and enhancement of law enforcement capabilities through appropriate legislative intervention.

6.7. To work with various OEMs/suppliers of Government Departments and Government agencies to ensure adequate cyber security measures and controls are built-into the products, services & operations rendered by OEMs/suppliers for Government applications and infrastructure.

6.8. To encourage the adoption of information security best practices by all entities and Stakeholders in the Government as well as Businesses, that is consistent with industry standards.

6.9. To review and adopt the latest threat management practices, principles and technology tools constantly, with the aim of achieving maturity in cyber security management & operations and to follow a risk-based approach for evaluating security controls.

6.10. To build security capabilities and infrastructure to provide layered protection for Government critical IT infrastructure, mission-critical systems and data.

6.11. To establish an institutional mechanism for continuous monitoring of the Government's IT infrastructure including endpoints.

6.12. To establish and/or strengthen Security Operation Centre (SOC) for all the Government critical IT infrastructure projects for obtaining strategic information regarding incidents, threats reported as part of the infrastructure and its system by creating incident response, crisis management through effective, predictive, preventive, protective, response and recovery actions on 24/7 basis.

6.13. To promote awareness of cyber security basics and encourage the adoption of secure practices within Government and its related workforces.

6.14. To create skilled staff workforce in cyber security across the Government Departments and Organizations through capacity building, skill development and training.

6.15. To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizens' data and for reducing economic losses due to cybercrime or data theft.

6.16. To engage information security professionals/organisations to assist e-Governance initiatives and ensure conformance to security best practices.

6.17. To encourage research, innovation & collaboration with industries and start-ups in the field of cyber security.

6.18. To promote Public Private Partnerships (PPP) with industry leaders, financial institutions and internet service providers to collectively strengthen cyber security posture of the State.

6.19. To conduct periodic audit of IT infrastructure and applications of the Government Departments to assess compliance to the cyber security controls and to prevent cyber-attacks. The society under DIT to engage (or act as) CERT-In empanelled agencies to conduct the audits, while simultaneously strengthening in-house capabilities by building a required team.

7. FOUNDATIONAL PRINCIPLES

The cyber security policy of Tripura is anchored in the foundational principles of Confidentiality, Integrity and Availability (CIA) ensuring a robust and trustworthy digital environment for the Citizens, Businesses and Government.

7.1. **Confidentiality:** Only authorized individuals or systems shall access sensitive data. Techniques such as encryption, access controls, data masking and anonymization, secure communication protocols and data classification and handling are to be used to protect confidentiality.

7.2. **Integrity:** Data should remain accurate, consistent, intact, uncorrupted and trustworthy throughout its lifecycle. The key strategies such as data encryption, access controls, data validation, hash functions, change management and digital signatures should be used to maintain the integrity and to prevent unauthorized alterations.

7.3. **Availability:** Availability of systems and data to authorize users shall be ensured by mitigating service disruptions caused by cyber-attacks or technical failures. The key aspects are preventing downtime, resilience, redundancy and Standard Operating Procedure (SOP) based incident response.

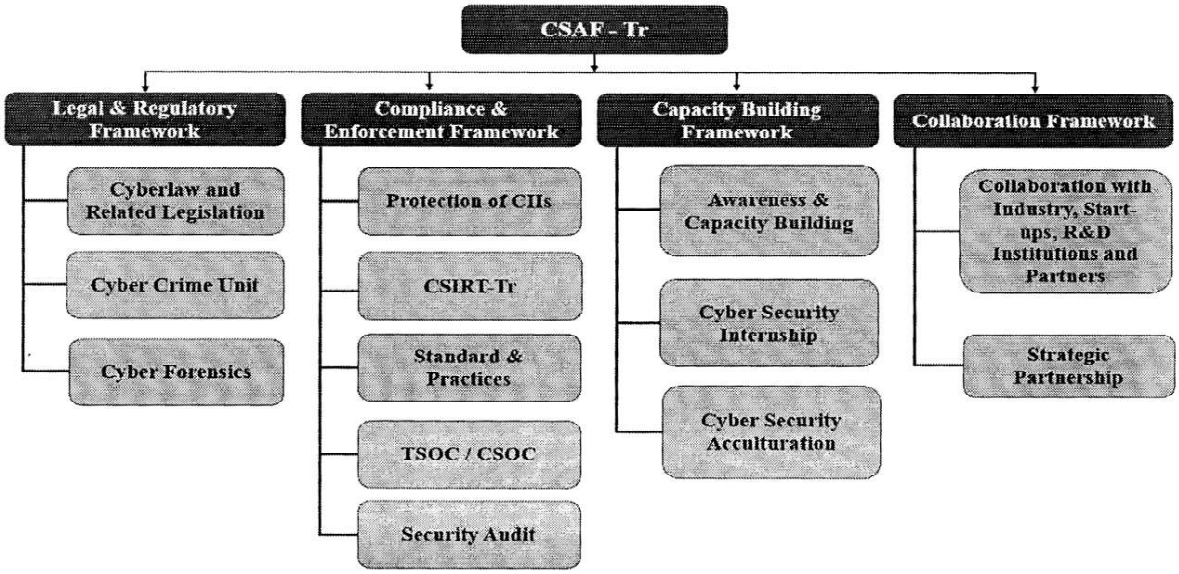
8. CYBER SECURITY ARCHITECTURE FRAMEWORK–TRIPURA

The Cyber Security Architecture Framework of Tripura (CSAF-Tr) defines the overall ambit of the Cyber Security related Bodies / Agencies in Tripura. The Cyber Security Architecture of Tripura (CSAF-Tr) shall be executed by the society under DIT. The major components that constitute the CSAF-Tr are:

A. Legal & Regulatory Framework
B. Compliance & Enforcement Framework
C. Capacity Building Framework
D. Collaboration Framework

RESTRICTED DOCUMENT

The Cyber Security Architecture Framework encompasses several other frameworks intended to provide a holistic and comprehensive solution in the field of cyber security. The four components that support the State's objectives in the cyber security policy are as follows:



The CSAF-Tr is an overall framework that allows the Government Departments to access Central Resources for Audit, Compliance, Incident Handling Assistance and Monitoring without hampering their unfettered ownership and handling of their resources. It is emphasized that while Policy remains consistent, several aspects of the Architecture will be dynamic in adapting to technological changes, regulatory requirements and Policies/Guidelines/mandates issued by MeitY, CERT-In and other related agencies from time to time.

9. STATE LEVEL CYBER SECURITY STEERING COMMITTEE

The SLCSSC shall provide high-level strategic oversight, guidance and coordination for the implementation of cyber security policies across all State Government Departments/Organizations/Agencies. It shall also ensure alignment with national policy frameworks, promote inter-Departmental collaboration and monitor the effectiveness of cyber security initiatives. The SLCSSC shall be constituted with the following members:

a)	Chief Secretary of Tripura	Chairman
b)	Director General of Police, Tripura	Member
c)	Principal Secretary / Secretary, IT, Govt. of Tripura	Member
d)	Principal Secretary / Secretary, Finance, Govt. of Tripura	Member

e)	Principal Secretary / Secretary, Law, Govt. of Tripura	Member
f)	Director, IT (CISO), Govt. of Tripura	Member Secretary
g)	Director, SFSL, Govt. of Tripura	Special Invitee
h)	Superintendent of Police, Cyber Crime, Govt. of Tripura	Special Invitee
i)	State Informatics Officer, NIC Tripura	Special Invitee
j)	Representatives of CERT-In	Special Invitee
k)	Any other technical officer deemed fit by CISO	Member

The SLCSSC shall establish a centralized governance mechanism to ensure accountability, consistent policy enforcement and strategic alignment of cyber security efforts, enabling a secure and resilient digital ecosystem for Citizens, Businesses and Government.

9.1. **Roles and Responsibilities of SLCSSC**

The SLCSSC shall be responsible for strategic oversight, coordination and governance of all cyber security initiatives in the State. Its core responsibilities include:

9.1.1. Review of the Cyber Security Policy and recommend for changes/ modifications if required.

9.1.2. Conducting periodic meeting to identify risks associated with IT infrastructure and applications of the State and mechanism to deal with mitigating the risks.

9.1.3. Setting up incident management response plan for the State.

9.1.4. Recommend for funding for effective implementation of cyber security policy.

9.1.5. Approve all policy matters related to Information Security and changes thereto.

9.1.6. Approve exceptions on a case-by-case basis when the requirements of the cyber security policy cannot be met, provide a timeline for the exception and follow-up the exception condition till the Security Policy requirements are met.

9.1.7. Review status of Cyber Security implementations and Audits.

9.1.8. Review of the compliance to the relevant laws including IT Act and also provide inputs for formulation of State legal frameworks for cyber security.

9.1.9. Formulating Cyber Crisis Management Plan (CCMP) for the State.

9.1.10. Overseeing the Data Recovery (DR)/Business Continuity Plan (BCP) implementation/operations of line Departments of the State through CSIRT-Tr/society under DIT.

9.1.11. Empowering the CISO of the State Government (i.e., Director, IT, Govt. of Tripura) to take necessary actions to strengthen the cyber security posture of the State and policy deviations reported/noticed.

10. ENTITIES AND RESPONSIBILITIES

10.1. Directorate of Information Technology (DIT)

The DIT, Government of Tripura shall be the Nodal Department for overseeing the IT Security of the State. DIT shall have the following roles with respect to cyber security:

10.1.1. Provide safe hosting for Servers, Applications, Websites and Data of various Departments.

10.1.2. Provisioning of secure network, monitoring network's security and responding to security alerts.

10.1.3. Advise all Government Departments/Directorates/Organisations/PSUs/ Statutory Bodies who are procuring IT/ICT Equipment and Services on technical aspects in general and security aspects in particular.

10.1.4. Establish and operate Cyber Security Architecture Framework (CSAF-Tr) including the Cyber Security Operations Centre (CSOC) and Computer Security Incident Response Team-Tripura (CSIRT-Tr). However, the functioning of Cyber Crime Unit and TSFSL shall be under the responsibility of Home Department, Govt. of Tripura.

10.1.5. Act as a Nodal Agency for carrying out Training and Capacity Building Programmes for Citizens, Businesses and Government on Cyber Security.

10.1.6. Formulate and issue Cyber Security related Policies/Guidelines/SOPs for the Government of Tripura. It will also formulate and put up recommended statutory framework for ensuring legal backing of the Policies.

10.2. Other Departments

10.2.1. All Government Departments are responsible for their IT assets. This includes services, Software and Hardware under their control.

10.2.2. Maintain a Software Bill of Materials (SBOM) for all software applications developed, procured or deployed, to ensure transparency, enable effective vulnerability management and enhance supply chain security in line with directives issued by MeitY, CERT-In or other competent authorities.

10.2.3. All the Head of the Departments (HoD) shall be nominated as Information Security Officer (ISO) for their respective Departments/Directorates/ Organisations/PSUs/Statutory Bodies.

10.2.4. All the Head of the Departments (HoD)/ISO shall seek advice from DIT for procurement of any IT/ICT equipment and services on technical as well as security aspects.

10.2.5. The Head of the Departments, being ISO, bears the overall responsibility for security of their assets and shall nominate an officer as Deputy Information Security Officer (Dy. ISO), who will be given training to identify and secure their assets and utilise the security directions/advisories given by the cyber security related Bodies/Agencies in Tripura effectively.

10.2.6. All the Departments/Directorates/Organisations/PSUs/Statutory Bodies shall extend necessary support as and when requested by DIT, being the Nodal Department for overseeing the IT Security of the State.

10.2.7. All the Departments/Directorates/Organisations/PSUs/Statutory Bodies in Government whoever implementing IT and ICT Projects shall earmark 1% to 3% of their annual Budget towards compliance as per IT Act 2000/2008, National Cyber Security Policy 2013 and this policy and with the security requirements to utilize the same for meeting the cost associated with the preparation and implementation of cyber security plans, procuring products required to provide cyber security for the information and assets, conducting joint training programs on cyber security and for conducting comprehensive security audit of systems/applications required under this policy.

10.2.8. The ISO/Dy. ISO of the concerned Departments/Directorates/ Organisations/PSUs/Statutory Bodies shall be responsible for any non-compliance in implementation/execution of relevant clauses mentioned in this policy.

10.2.9. All Departments/Directorates/Organizations/PSUs/Statutory Bodies shall ensure the hardening of IT infrastructure by implementing appropriate measures and conducting periodic vulnerability assessments and penetration testing.

11. LEGAL & REGULATORY FRAMEWORK

The objective of the legislative framework is to address specific legislation governing cyberspace activity through various collaborative initiatives. The State may collaborate

with legal experts in the area of cyber security to study the existing legal frameworks, identify problems and formulate advocacy laws to tackle real-time issues. This collaborative effort will be given the needed impetus to counter the ever-evolving nature of cyber threats, crime and piracy.

11.1. Cyber Crime Unit

A specialized Cyber Crime Unit under Tripura Police Crime Branch, was established for investigating into complaints pertaining to offences under the Information Technology Act. The Government shall further focus on enhancing and strengthening this unit in terms of infrastructure, tools & technologies such as advanced digital forensic tools & mobile forensic kits, malware analysis & crypto tracing capabilities etc. and specialized manpower to simplify reporting, tackling and tracking progress on cybercrimes, ensuring its continuous upgradation to effectively address issues pertaining to cyber-crimes. Further, State Government has established a Cyber Crime Police Station to deal with the cases related to Cyber Crime. The existing Cyber Crime Police Station may be further strengthened by setting up a mini cyber forensics lab.

11.2. Cyber Forensics

The State has established a digital forensics division in the TSFSL under Home Department, Govt. of Tripura to analyse and investigate cybercrime to assist in the data recovery, analysis and preservation of digital evidence as well as to recover corrupted and deleted data that are not available for intended use as a result of cybercrime. In line with capacity building efforts, the State should further focus on upgrading advanced digital forensic tools & mobile forensic kits, malware analysis & crypto tracking capabilities etc. alongwith strengthening the data recovery mechanisms and also improve evidence preservation standards. The State should also take necessary steps in line with Section 79A of the Information Technology Act, 2000, which empowers the Central Government to notify the State Forensic Science Laboratory as the "Examiner of Electronic Evidence". A digital evidence preservation facility shall also be created to have a secure environment for retention of digital evidence. Additionally, strategies should be outlined for skill development, adopting emerging technologies and collaborating with cyber security experts and law enforcement agencies. Regular comprehensive audits and reviews will help identify gaps and ensure continuous improvements to combat advanced cybercrimes effectively.

RESTRICTED DOCUMENT

12. COMPUTER SECURITY INCIDENT RESPONSE TEAM-TRIPURA

The Government shall set up Computer Security Incident Response Team-Tripura (CSIRT-Tr), a nodal Body/Agency for the State to coordinate with different Government Departments, Directorates, institutions, organizations and companies. The CSIRT-Tr shall contribute towards the State's efforts for a safer, stronger Internet for all citizens by responding to major incidents, analysing threats and exchanging critical cyber security information with trusted partners. The Departments/PSUs/ Organisations/ Agencies under Government of Tripura may establish their own sectoral CSIRT based on the threat profiles, assets, operational technologies and risk landscapes associated with their IT infrastructure, in line with the policies and guidelines issued by their respective Ministries in the Government of India and shall coordinate closely with the CSIRT-Tr for incident reporting, threat intelligence sharing and response activities. The primary mandates of CSIRT-Tr would be to:

12.1. Provide cyber security related actionable information to the Government, critical infrastructure agencies, private industries and general public through advisories.

12.2. Provide cyber security protection through intrusion detection and prevention capabilities.

12.3. Develop State's Cyber Crisis Management Plan (CCMP)/framework and implement the same in coordination with CERT-In, offering the following services to critical infrastructure clients:

12.3.1. Assist the State in collaborative efforts to improve the cyber security posture of the State.

12.3.2. To ensure proactive sharing of information/incident log/intel with all other relevant stakeholders like CERT-In, NCIIPC, NCCC and Sectoral CSIRTs (if any), ISOs/Dy. ISOs of concerned Departments etc.

12.3.3. Act as a nodal Body / Agency to conduct comprehensive security audits or assessments of State Government and constituent IT infrastructure in the State in line with evolving security policy for the State. A dedicated officer of the nodal Body / Agency shall coordinate with stakeholders and drive the State's efforts. Further, a round the clock support facility will be established for emergency response and crisis management through a network of dedicated officers in every Department. The support team shall continuously monitor the cyber situation in the State.

12.3.4. Initiate proactive measures to increase awareness and understanding of information security and computer security issues.

12.3.5. Implement mandatory cyber drills and exercises for Government entities and critical infrastructure.

12.4. The SLCSSC shall decide and finalize the administrative composition/ organizational structure of CSIRT-Tr and empower the Director, IT, Govt. of Tripura to function as the Head and Apex Authority of CSIRT-Tr.

13. CRITICAL INFORMATION INFRASTRUCTURE (CII)

13.1. All CIIs of the State of Tripura needs to be identified jointly with NCIIPC and to be notified in the official gazette as "Protected System" under Section 70 of IT Act 2000.

13.2. Any attack on a "Protected System" with intent to threaten the unity, integrity, security or sovereignty of the nation or to strike terror in the people or any section of the people, shall be treated as Cyber Terrorism (Section 66F of IT Act 2000). Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

13.3. Critical assets are the specific resources which are most vital for financial systems, healthcare systems, emergency services systems, transportation, utility services and telecommunications.

13.4. Critical assets/applications include data, systems, networks, physical infrastructure, people and third-party contracts (vendors, developers, system integrators and other partners).

13.5. Comprehensive risk assessment to be done by the Departments through their ISOs/Dy. ISOs to identify and define criticality by evaluating the value, sensitivity, and potential consequences of compromise for each asset/application. The Departments/System Integrators shall comply to the standards/processes established by cyber security related bodies/agencies/organizations of the State and national level.

13.6. The Department/System Integrator shall employ the strategies like secure architecture design, authentication & authorization, data encryption, secure Software Development Life Cycle (SDLC), patch management, incident response plan, security awareness etc.

13.7. The Departments shall share the information of all IT infrastructure/critical assets/applications with CSIRT-Tr/society under DIT annually or as and when added afresh. CSIRT-Tr/society under DIT shall carry out random/periodical checks in this regard.

13.8. CSIRT-Tr/society under DIT shall develop mechanisms to facilitate sharing of information on security breaches, incidents, cyber-attacks, espionage etc. among CII stake holders, as well as with Central agencies dealing with cyber security.

13.9. CSIRT-Tr/society under DIT shall also access the critical assets/applications through its internal cyber security team to ensure the stability and security of the system.

13.10. CSIRT-Tr/society under DIT shall carry out regular comprehensive Information Security Audit and Penetration Testing for mitigating Cyber Security incidents. The observations reported shall be immediately addressed by the concerned asset owners.

13.11. In the event of any major threat/vulnerability identified on these critical assets/ applications and if not resolved within a reasonable time, CSIRT-Tr/society under DIT is empowered to shut down or take-out the application from the network until resolved.

14. ESTABLISHMENT OF CYBER SECURITY STANDARD AND PRACTICES

All the Departments/PSUs/Organisations/Agencies under Government of Tripura shall adopt the following Cyber Security Standards and Practices:

14.1. Strive to implement Information Security Standards/Guidelines and Best Practices to ensure compliance with recognized industry standards.

14.2. The implementation of Information Security Standards/Guidelines to be reviewed, approved and kept up to date to support incident handling and response activities.

14.3. Joint development of a State Cyber Crisis Management Plan to protect State information, assets and critical infrastructure.

14.4. Identity and Access Management (IAM) will be implemented to secure patch management processes, protect sensitive data and ensure that access to systems and infrastructure is authorized, auditable, and periodically reviewed.

14.5. To conduct scheduled cyber security policy reviews to address emerging threats.

14.6. To prioritize cyber security measures based on risk assessment and criticality.

14.7. To ensure high levels of transparency and collaboration at various levels, the Government shall promote use of open standards and data exchange.

14.8. In reference to the clause 10.2.3 of this policy, ensure security certification on procurement of IT security product/critical IT infrastructures/services. Any product/service blacklisted by Government of India for cyber security reasons should be complied under this policy.

14.9. To adopt secure Software Development Life Cycle (SDLC) to incorporate security as a key component of the software/application development process

ensuring compliance with global standards, build software with robust security measures, reducing the likelihood of security breaches, protecting sensitive data and delivering secure and reliable software/application.

14.10. **Security Audit:**

14.10.1. Departments/Organizations should ensure that all Government websites, web applications, mobile apps, APIs etc. mandatorily undergo and clear a comprehensive Security Audit carried before being hosted in the State Data Centre.

14.10.2. Third party Security audit must be conducted by CERT-In empanelled auditor periodically for all websites, web applications and APIs etc. Additionally, a fresh audit should be carried out if there are changes in dynamic content, discovery of new vulnerabilities, or expiry of the existing audit certificate whichever occurs first. Further, internal Security Audit to be performed at least once in six months.

14.10.3. DIT shall engage CERT-In empanelled agencies to conduct the audits, and the concerned Department/Directorate/Organization under Government of Tripura intends to conduct security audit of their website/web application/mobile app shall submit request for conducting security audit to DIT only through the SAaaS portal (https://saaas.tripura.gov.in).

14.10.4. In addition to engagement of CERT-In empanelled auditors, DIT/society under DIT shall develop a mechanism to simultaneously strengthen its in-house auditing capabilities by building a required team.

14.11. **Hosting Policy:**

14.11.1. Ensure all e-Governance applications and / or its related infrastructure are hosted at TSDC or concerned Departments on-premise Data Centre. For secure operations of TSDC, a detailed guideline on Web Hosting and Co-Location process to be issued for seamless hosting process and activities for hosting the User Department's Web applications, websites and infrastructure.

14.11.2. Applications owned by Departments shall mandatorily have the certificate of safe hosting provided by the third-party CERT-In empanelled auditor.

14.11.3. While the equipment is located in the co-location facility, the owner Department is responsible for insuring, maintaining their equipment,

providing cover against any risk of failure of the equipment. CSIRT-Tr/society under DIT shall perform joint review of the same quarterly.

14.12. **Backup and Recovery**

14.13.1. Every Department, while hosting application in the State Data Centre, shall mandatorily list out the folders, databases and logs that need to be backed up with the periodicity (daily/weekly/monthly/yearly) mentioned.

14.13.2. The Department shall ensure that the backed-up datasets/databases are stored in tapes/external devices or in servers/storage in more than one location other than the primary space of storage.

14.13.3. The backed-up datasets shall be restored periodically and confirmed by the concerned Department for the correctness and completeness.

14.13.4. CSIRT-Tr/society under DIT shall conduct a random audit of Government applications/infrastructure for backup and recovery process.

14.13.5. Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction.

15. TRIPURA SECURITY OPERATION CENTRE / CYBER SECURITY OPERATIONS CENTRE

DIT has established a dedicated Security Operation Centre (SOC) and in line with capacity building efforts, the State should further focus on upgrading the existing SOC to CSOC to enable proactive monitoring, detection, response and mitigation of cyber threats targeting Government digital infrastructure. It shall operate in close coordination with CSIRT-Tr to facilitate real-time incident response, seamless threat intelligence sharing, and alignment with national cyber security policies and frameworks. The primary roles and responsibilities are:

15.1. To monitor all Government IT infrastructure for intrusions/incidents through various Cyber Security tools and raise suitable alert.

15.2. To perform Vulnerability Assessment and Penetration Testing (VAPT) of all Government applications and infrastructure.

15.3. To provide solution document/guidance to the Departments for identified vulnerabilities.

15.4. To provide mitigation measures on cyber incidents / intrusions for affected systems.

15.5. To conduct mock drills, exercises and bug bounty programs periodically for the applications of the Government Departments.

16. CAPACITY BUILDING FRAMEWORK

16.1. Awareness and Capacity Building

16.1.1. Advise public on safe practices and improve awareness.

16.1.2. Promote and launch a comprehensive State awareness program on security of cyberspace.

16.1.3. Identify Master Trainer for each Department for training on cyber security.

16.1.4. Capacity building of Departmental technical staff/developers on secure software/application development.

16.1.5. Encourage, develop or impart training to increase cyber security awareness at all levels.

16.1.6. Build a strong workforce of auditors, policy implementers, data management experts, forensic personnel, penetration testers and cyber security experts to provide cyber security related services.

16.1.7. The month of October shall be observed annually as Cyber Security Awareness Month across the State, featuring coordinated initiatives, training sessions and public engagement activities aimed at enhancing cyber hygiene and promoting a culture of security among Government, Businesses and Citizens.

16.1.8. Joint cyber mock drills involving critical infrastructure agencies, the police, CSIRT-Tr and TSOC/CSOC shall be conducted annually to test the cyber incident response readiness of the State.

16.2. Cyber Rakshak Internship Program

A platform will be established to provide internship opportunities named "Cyber Rakshak Internship Program" which will enable undergraduate students to gain practical exposure, enhance their skills and connect with industry for future career growth. A stipend of Rs.5000/- per month (for upto 3 months) will be provided to 100 engineering undergraduates interns, domiciled in the State, per year for successful internships in the cyber security domain. A committee under DIT shall be constituted for selection and recommendation of students as well as disbursement of stipends.

16.3. Cyber Security Acculturation

16.3.1. The Government shall launch a state wide multi-channel awareness campaign involving workshops, social, print and digital media etc. to create cyber security awareness among citizens.

16.3.2. The Government shall announce an annual competition, named like Cyber Surakshit Tripura Hackathon, involving technical partners/ institutions that will help identify and nurture individual talent. This will be a state wide drive to increase awareness as well as build assurance in the community about Government initiatives and efforts to secure the cyberspace with the help of its stakeholders. This challenge will have different levels of complexity to appeal to personnel of varying levels of cyber security skills and competency.

16.3.3. The State shall issue live document guidelines on best practices to help citizens and organizations stay aware of the latest developments in cybercrime and address them proactively.

16.3.4. Inputs on cyber security education and awareness shall be introduced as part of the State's school and college curriculum to equip students with knowledge of safe digital practices, promote cyber hygiene, and develop a basic understanding of cyber threats and their prevention.

17. COLLABORATION FRAMEWORK

17.1. Collaboration with Industry, Start-ups, R&D Institutions & Partners

17.1.1. The State shall set up a Centre of Excellence (CoE) with the support from Government of India or its agencies or from any expert organizations to boost research in the field of cyber security. The State shall also launch specific R&D projects relevant to current day challenges that the Government faces, which will be addressed through the CoE. State Government shall associate or collaborate with any institution/knowledge partner/technical partner in this respect through nodal agency/body.

17.1.2. For R&D projects in the domain of cyber security, driven by Tripura-based industries or start-ups, reimbursement of up to a maximum of 50% of the total project R&D cost, or up to Rs.1.0 lakh, whichever is lower shall be provided to Tripura-based industries or start-ups. These grants may be availed by an entity once over the policy period. Maximum five such projects will be funded in each year.

17.1.3. Reimburse the cost up to a maximum of Rs.50,000/- towards engagement of CERT-In empanelled service providers by start-ups registered with Tripura Start-up Cell for cyber security audit, incident management and incident response activities. This may be availed by Tripura based start-ups once over the policy period and on submission of necessary documentary evidences and invoices/bills. This benefit will be provided to 10 eligible Tripura based start-ups each year.

17.2. **Strategic Partnership**

17.2.1. The Government shall enter into strategic partnerships with the private sector to set up infrastructure such as cyber security training and development labs, which in turn will facilitate the development of new products.

17.2.2. The Government shall strive to enter into strategic alliances with international institutions/agencies to benefit from their infrastructure, skill set and research capabilities.

18. PRIORITIZED APPROACH FOR IMPLEMENTATION

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

19. OPERATIONALISATION OF THE POLICY

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as State, Department, as may be appropriate, to address the challenging requirements of security of the cyberspace.

20. POLICY PERIOD

The Tripura Cyber Security Policy 2025 will remain in operation from the date of its notification until substituted by another policy. This policy shall supersede all the prior policies in this subject.

RESTRICTED DOCUMENT

21. ANNEXURE A

Mapping of Tripura State Cyber Security Policy objectives with Strategies are outlined below:

Sl. No.	Objectives	Strategy as proposed in the Policy
1	To safeguard Government information assets including IT & ICT infrastructure, Operational Technology (OT), Industrial Control Systems (ICS), network, software and citizen services and ensure their maximum availability to the Citizens, Businesses and Government.	• Protection of Critical Information Infrastructure (CII) of the State. • Strengthening of TSOC/ CSOC.
2	To create a secure cyber ecosystem in the State and generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby encouraging adoption of secured IT and ICT infrastructure in all sectors of the economy of the State.	• Security must be an integral part of IT system implementation like following "secure by design" principle while building an application. • Follow security and rigor in IT operations and support.
3	To implement the Cyber Security Policy for Government of Tripura, under the suitable framework for promotion and enabling actions for compliance towards the national & global standards and best practices.	• Adoption and implementation of Cyber Security Architecture Framework–Tripura (CSAF-Tr).
4	To establish a nodal body for the State to coordinate with Departments, institutions, organizations & agencies which will contribute towards the State's efforts for a safer, stronger & trusted Internet for all citizens by responding to major incidents, analysing threats & exchanging critical cyber security information with trusted partners.	• Establishment and operationalisation of CSIRT-Tr.

RESTRICTED DOCUMENT

Sl. No.	Objectives	Strategy as proposed in the Policy
5	To strengthen the Legal and Regulatory framework for ensuring a secure cyberspace ecosystem and to foster cooperation and coordination with other cyber security agencies and institutions such as MeitY, CERT-In, NCIIPC, NCCC, I4C, NIC-CERT, Cyber Crime Unit, SFSL etc.	• Legal & Regulatory Framework under CSAF-Tr. • Establishment of CSIRT-Tr.
6	To enable effective prevention, investigation and prosecution of cyber-crime and enhancement of law enforcement capabilities through appropriate legislative intervention.	• Strengthening of Cyber Crime Unit and the Legal & Regulatory Framework.
7	To work with various OEMs / suppliers of Government Departments and Government agencies to ensure adequate cyber security measures and controls are built-into the products, services & operations rendered by OEMs/suppliers for Government applications and infrastructure.	• Align with OEMs and ISPs to ensure directions of regulatory agencies are adhered at the time of design.
8	To encourage the adoption of information security best practices by all entities and Stakeholders in the Government as well as businesses, that is consistent with industry standards.	• Cyber Security Acculturation
9	To review and adopt the latest threat management practices, principles, and technology tools constantly, with the aim of achieving maturity in cyber security management and operations and to follow a risk-based approach for evaluating security controls.	• Establishment of Cyber Security Standards and Best Practices.
10	To build security capabilities and infrastructure to provide layered protection for Government critical IT infrastructure, mission-critical systems and data.	• Security Infrastructure upgradation/augmentation of Critical Information Infrastructure (CII).

RESTRICTED DOCUMENT

Sl. No.	Objectives	Strategy as proposed in the Policy
11	To establish an institutional mechanism for continuous monitoring of the Government's IT infrastructure.	• Establishment and operationalisation of CSIRT-Tr. • Strengthening of TSOC/ CSOC.
12	To establish / strengthen Security Operation Centre (SOC) for all the Government critical IT infrastructure projects for obtaining strategic information regarding incidents, threats reported as part of the infrastructure and its system by creating incident response, crisis management through effective, predictive, preventive, protective, response and recovery actions on 24/7 basis.	• Strengthening and operationalisation of TSOC/ CSOC & CSIRT-Tr.
13	To promote awareness of cyber security basics and encourage the adoption of secure practices within the Government workforce.	• Capacity Building Framework
14	To create skilled staff workforce in cyber security across the Government departments and Government agencies through capacity building, skill development and training.	• Capacity Building Framework
15	To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft.	• Foundational Principles • Protection of Critical Information Infrastructure (CII) of the State. • Strengthening of Cyber Crime Unit and the Legal & Regulatory Framework.
16	To engage information security professionals/organisations to assist e-Governance initiatives and ensure conformance to security best practices.	• Establishment and operationalisation of CSIRT-Tr & TSOC/CSOC.
17	To encourage research, innovation and collaboration with industries and start-ups in the field of cyber security.	• Collaboration Framework

RESTRICTED DOCUMENT

Sl. No.	Objectives	Strategy as proposed in the Policy
18	To promote Public Private Partnerships (PPP) with industry leaders, financial institutions and internet service providers to collectively strengthen cyber security posture of the State.	• Collaboration Framework
19	To conduct periodic audit of IT infrastructure and applications of the Government Departments to assess compliance to the cyber security controls and to prevent cyber-attacks. DIT/society under DIT to engage CERT-In empanelled agencies to conduct the audits, while simultaneously strengthening in-house capabilities by building a required team.	• Establishment of Cyber Security Standard and Practices • Establishment and strengthening of CSIRT-Tr & TSOC/CSOC.

*****